The Use of Multi-Layered, Conditionally EM-Permissive Nanostructures to Support Jamming-Resistance Through Time-Specific Analysis of Received Signals in Contested Environments

12 September 2023

Simon Edwards
Research Acceleration Initiative

Introduction

A challenge facing materials scientists at this time is overcoming the paradox of the need to block electromagnetism from jamming sources whilst allowing legitimate signals to pass through materials meant to block these unwanted signals. Great strides have been made within the past six years in developing highly effective, ultra-thin metamaterial bi-layers capable of blocking electromagnetism.

Abstract

The creative use of these materials may enable the creation of purpose-built nanostructures that permit the flow of signals through a multi-layered structure wherein only when a security key is transmitted immediately ahead of the proper signal.

These nanostructures would be interchangeable coverings for communications ports, most likely primarily used on drone aircraft, but conceivably also utilized in data centers in which one wishes to employ discrete, air-gapped traffic authentication mechanisms in which even an entity that has already gained full system access would be unable to determine the proper key that enables access to the system. Their interchangeability would enable rapid response to the compromise of authentication keys and their replacement with new keys.

Each layer would be composed of WSe2 and MoS2 in their respective layers with a series of semiconductor elements shaped, essentially, like a flat paint chip acting as a bridge between WSe2/MoS2 bi-layers. The EM-blocking bi-layers would be doped with the semiconductor flakes with each of those flakes having the characteristic of being flat, whilst having a uniformly angled orientation known only to the designer. This angling would result in the induction and retransmission of signal between layers provided that the frequency of the energy exactly matched the "apparent" width of the flake. These angular differences could be as subtle as a single degree of rotational difference or could be as coarse as a binary "horizontal" vs. "vertical" orientation. With a sufficient number of layers, even a binary number of possible orientations could form the basis of a robust and secure gating system provided 40-50 layers of either horizontal or vertical orientations in a unique combination known only to the legitimate user of the system.

Even in a jamming-heavy environment, by comparing the received signals in the post-unlock window (let's say this is 1.5 microseconds, for the sake of argument) of three re-transmissions to one another, the authentic signal could be deduced through an automated analytical method given that only a legitimate source would be likely to be sending legitimate unlock signals, the proper signal cannot be bruteforced and as three redundant transmissions of the legitimate instruction set would provide ample data for an advanced system to perform a real-time comparative analysis of signals received during the unlock windows in order to separate signal from noise.

The strength of the system, rather than lying in blocking all unwanted signals and allowing desired signals, lies in the ability to block nearly all of the illegitimate signals most of the time and providing an analytical starting point that is valuable for the same reason that asking someone to repeat themselves a sufficient number of times in a noisy room can enable one to deduce the intended message despite having no means of blocking the noise. The unlock signal itself cannot be jammed since the mere presence of EM in the correct combination of frequencies (and in the correct timing) would be interpreted by the system as an "authentication" without regard to the presence of other signals. No analysis is required in this system to determine what is or is not an authentication signal since this work is done entirely by a solid-state nanostructure and not by the computer. By giving a platform the critical piece of information of "when" a legitimate signal starts and ends without it needing to actually properly hear the signal, drone aircraft may therefore operate in even the most intensely contested EM environments.

Conclusion

Despite speculation to the contrary, it is not likely that it will ever be considered wise or practical for decisions concerning lethal action to be controlled by onboard artificial intelligence, meaning that it will remain very much necessary to continue to develop novel methods to enable resistance to jamming.